REMARKS

Claims 1-4, 6, 8, 10-21, 23, 25, 27-38, 40, 42, and 44-51 are pending.

Previous Rejections

Applicant notes and appreciates withdrawal of the previous rejections.

New Claim Rejections

In the present Office Action, claims 1-3, 6, 8, 10-12, 15-16, 18-20, 23, 25, 27-29, 32-33, 35-37, 40-42, 44-46, and 49-50 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,167,052 (hereinafter "McNeill"), in view of U.S. Patent No. 6,584,069 (hereinafter "Kagemoto"). Claims 4, 13, 21, 30, 38, and 47 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over McNeil and Kagemoto, in further view of U.S. Patent No. 6,424,626 (hereinafter "Kidambi"). Finally, claims 14, 17, 31, 34, 48, and 51 are rejected under 35 U.S.C. § 103(a) as being unpatentable over McNeil and Kagemoto, in further view of U.S. Patent No. 6,266,773 (hereinafter "Kisor"). Applicant has carefully considered the new rejections and believe patentably distinctions exist. Therefore, Applicant respectfully traverses the rejections and requests reconsideration.

Regarding each of independent claims 1, 18 and 35, paragraph 4 of the present Office Action suggests McNeill discloses most of the features recited. However, as discussed below, McNeill does not disclose the features as suggested.

It is first noted that the portions of McNeill cited in paragraph 4 of the Office Action generally describe how an access control list for a router may be created. For example, the following portion of McNeill is cited as disclosing the features "determining a first incoming packet community set (PCS) of a first data packet received on an interface of said firewall":

> "Step A1 creates lines that allow traffic to the interface 210 from each shared subnet such as subnet 116S. The program writes to the access control list the words "access-list", the access control list number (generated sequentially by the program itself in some embodiments), the words "permit ip", the IP address of the shared subnet, and the wildcard-mask of 0.0.0.255. (A 0 bit in the wildcard-mask indicates that the corresponding bit of the source IP address is used by the router in comparisons with incoming packet IPs; a 1 bit in the wildcard-mask indicates that the corresponding bit is not used.)
>
> The wildcard-mask 0.0.0.255 in line AL1-1 is determined by inverting the subnet mask.
>
> Step A2 creates lines, such as lines AL1-2a, AL1-2b, which allow traffic from every other subnet (i.e. layer 2 BD) in the same connectivity group. Line AL1-2a allows traffic from subnet 10.1.2.0/24 (VLAN 140b). Line AL1-2b allows traffic from subnet 10.3.2.0/24 (VLAN 140h).
>
> Step A3 creates line AL1-3 denying traffic from all the other stations in network 110. (Of note, when the router receives a packet, the router tests the packet starting from the beginning of the access control list. When a line that applies to the packet is found, the rest of the access control list is ignored.) The wildcard-mask is obtained by inverting the IP address range mask of network 110." (McNeill, col. 8, line 50 – col. 9, line 7).

However, as seen from the above, the disclosure describes creation of the access control list and does not describe operation of the router. Therefore, the cited portion does not disclose "determining a first incoming packet community set (PCS) of a first data packet received on an interface of said firewall." Nevertheless, putting aside these distinctions for the moment, other features of the claims are not found in the reference as discussed below.

Additionally, McNeill discloses IP based access control lists. Therefore, matching of a received packet to such a rule is based on an IP address of the received packet. Claim 1 recites the features:

> "determining a first incoming packet community set (PCS) of a first data packet received on an interface of said firewall;
>
> discarding said first data packet in response to detecting said first incoming PCS is not a subset of an interface community set (IFCS) of said interface."

With respect to inter-domain communication, McNeill discloses the following:

> "Stations in different layer 2 domains (e.g. stations 124.1, 124.3) cannot communicate with each other using exclusively MAC addresses. They communicate using their IP addresses which are logical addresses. Routers 130.1, 130.2, 130.3 route traffic between the domains 116 based on the stations' IP addresses, translating between IP addresses and MAC addresses as needed." (McNeill, col. 1, lines 47-53).
>
> "As stated above, communications between different domains use IP addresses. For example, to send a packet to station 124.3, station 124.1 inserts into the packet the IP address of station 124.3 and the MAC address of router 130.1 as the logical and physical destination addresses, respectively. Router 130.1 replaces the destination MAC address with the MAC address of router 130.2 and replaces the source MAC address of station 124.1 with the MAC address of router 130.1. Then router 130.1 sends the packet to router 130.2. Router 130.2 replaces the source MAC address in the packet with its own MAC address and the destination MAC address with the MAC address of station 124.3, and sends the packet to switch 128.3. Switch 128.3 forwards the packet to station 124.3 through switch 128.5." (col. 3, lines 40-53).

Assuming for the sake of argument (it is not explicitly disclosed) the router translates the MAC address of the sending station (124.1) to a corresponding IP address, the router may then compare the incoming packet to an access control list rule. Assuming this scenario, claim 1 recites the additional features:

> "matching said first data packet to a first rule of a plurality of rules of said firewall;
> comparing said first incoming PCS to a second incoming PCS specified by the first rule;
> changing the first incoming PCS in the first data packet to an outgoing PCS specified by the first rule, in response to determining the first incoming PCS matches the second incoming PCS;
> comparing said outgoing PCS with a destination community set of said first data packet, prior to transmitting the first data packet to said destination community;
> discarding said first data packet in response to detecting said outgoing PCS is not a subset of said destination community set; and
> further processing said first data packet in response to detecting said outgoing PCS is a subset of said destination community set."

On page 3 of the Office Action, it is suggested the following from McNeill discloses the above features:

> "Stations in different layer 2 domains (e.g. stations 124.1, 124.3) cannot communicate with each other using exclusively MAC addresses. They communicate using their IP addresses which are logical addresses. Routers 130.1, 130.2, 130.3 route traffic between the domains 116 based on the stations' IP addresses, translating between IP addresses and MAC addresses as needed." (McNeill, col. 1, lines 47-53).

> "Step A4 creates the line AL1-4 allowing traffic from any station outside the network 110, including traffic from the Internet 170. In some embodiments, before step M50 the administrator indicates to management station 124M, for each subnet in a connectivity group, whether the traffic from the Internet to the subnet is allowed. If the traffic is denied, step A4 is omitted for the corresponding interface, and step A3 creates a "deny ip any" line instead of line AL1-3." (McNeil, col. 9, lines 8-15).

> "Some embodiments allow the network administrator to insert additional commands into the access control list. Thus, in some embodiments, before step M50, the administrator can specify for each subnet additional terms to be inserted into the access control list for the corresponding interface(s). More particularly, the administrator can specify terms to be inserted before step A, terms to be inserted between steps A2 and A3, terms to be inserted between steps A3 and A4, and terms to be inserted after step A4. In some embodiments, this

> technique is used to incorporate firewall functionality into the access control lists and thus eliminate the need for a separate enterprise-wide firewall." (McNeill, col. 9, lines 38-49).

It has already been established earlier in the claim that the first incoming PCS may be equated by the examiner with the source station IP address. Therefore, assuming for the sake of argument that the incoming PCS is equivalent to the first incoming PCS, McNeill does not then disclose "changing the first incoming PCS in the first data packet to an outgoing PCS specified by the first rule, in response to determining the first incoming PCS matches the second incoming PCS." Even assuming the translation of the source station's MAC address to a corresponding IP address, McNeill teaches making this change/translation before matching a given rule. Therefore, McNeill does not disclose changing the first incoming PCS to an outgoing PCS. specified by the first rule, in response to determining the first incoming PCS matches the second incoming PCS.

Additionally, it is noted that the claims recites "changing the first incoming PCS to an outgoing PCS <u>specified by the first rule, in response to determining the first incoming PCS matches the second incoming PCS</u>." Neither are these features disclosed by McNeill. The McNeill router is a router and is not configured to perform the features are recited in the claim. Other address translations disclosed by McNeill involve changing amongst router MAC addresses. However, as already discussed, such MAC addresses are not used for the access control lists and do not meet the claim features.

It's also noted that McNeill merely discloses that an administrator could insert commands to provide firewall functionality. However, such commands and functionality are not disclosed in McNeill.

For at least the above reasons, each of the independent claims are patentably distinct from the cited art, taken either singly or in combination. Accordingly, all of the pending claims are patentably distinguishable from the combination of cited art.

In view of the prosecution history of the present application, the below signed representative requests a telephone interview (512) 853-8866 in order to facilitate a resolution should the examiner believe the present rejections should be maintained.

CONCLUSION

Applicant submits the application is in condition for allowance, and an early notice to that effect is requested.

If any extensions of time (under 37 C.F.R. § 1.136) are necessary to prevent the above referenced application(s) from becoming abandoned, Applicant(s) hereby petition for such extensions. If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/5181-75900/RDR.

Respectfully submitted,

/Rory D. Rankin/

Rory D. Rankin
Reg. No. 47,884
ATTORNEY FOR APPLICANT(S)

Meyertons, Hood, Kivlin,
Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8800

Date: May 1, 2007